AIR WAR COLLEGE

AIR UNIVERSITY

FLEXIBLE OPTIONS FOR CYBER DETERRENCE

by

Frank W. Simcox, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

11 February 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Flexible Options For Cyber Deterrence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College Air University**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**47**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Biography

Lieutenant Colonel Frank W. Simcox is a student at the Air War College, Maxwell Air Force Base, Alabama. Lieutenant Colonel Simcox entered the Air Force in 1987 through the Reserve Officer Training Corps after graduating from Washington University, St. Louis, Missouri, with a Bachelor of Science Degree in Electrical Engineering. He is a 1994 graduate of The Eller College of Business and Public Administration, University of Arizona, Tucson, Arizona, where he earned a Master of Science Degree in Information Systems Management. Prior to his current assignment, he served as the commander of the 603d Air & Space Communications Squadron. The squadron is attached to the 603d Support Group, Ramstein Air Base, Ramstein AB Germany. As squadron commander, he served as the senior officer for more than 100 communications and information systems airmen. He was responsible for ensuring the squadron was prepared to support the 603d Air & Space Operations Center weapon system. Lieutenant Colonel Simcox subsequently served as the Chief, Plans and Resources Division, Directorate of Communications, Headquarters United States Air Forces in Europe (USAFE), Ramstein AB Germany. In this position, he was responsible for design, installation, and sustainment of USAFE's enterprise information systems and an annual budget of over $100 million. Lieutenant Colonel Simcox has held a variety of positions at squadron, major command, and joint levels.

Captured in the words of Sun-Tzu is the great advantage of deterrence, "attaining one hundred victories in one hundred battles is not the pinnacle of excellence, subjugating the enemy without fighting is the true pinnacle of excellence."[1]

Chapter 1

Introduction

This paper describes options for cyber deterrence to address both asymmetric threats from terrorists and the intimidation associated with nation-state peer competitors in the cyber domain. It presents recent National Security Strategy interests and demonstrates a lack of focus upon cyber infrastructure. The paper will examine challenges associated with legal aspects in the cyber domain as well as the issue of attribution. It will analyze terrorist and nation-state usage of cyberspace and potential threats aimed at the United States related to each. Finally, the paper concludes with several recommendations for tailored cyber deterrence focused on terrorists and peer nation-states.

The idea of deterrence has existed since the beginning of humanity. Lawrence Freedman in his book *Deterrence* uses the biblical tale of Adam, Eve, and the forbidden fruit as an example of deterrence.[2] Webster defines deterrence as "maintenance of military power for the purpose of discouraging attack."[3] The threat of war has always been a tool used by leaders to influence foreign powers to avoid acts of aggression. Ultimately, deterrence became synonymous with American Cold War strategic thinking and foreign policy.

Mutually assured destruction was a classic adoption of deterrence through punishment. However, deterrence through punishment requires the demonstration of offensive capabilities. The highly classified nature of the United States cyber-based offensive tools makes this approach unlikely. In addition, deterrence by punishment does not work without identification and

attribution. Lastly, any assumption of rationality demonstrates the fallacy of Cold War deterrence applied to the cyber domain.

Today's multi-polar world provides multiple threats aimed at the United States in the cyber domain. From cyber terrorists to sophisticated nation-states, adversaries are increasing their cyber capabilities on a daily basis. Some argue for an offensive cyber doctrine of preemption, but as demonstrated in Iraq, preemption can be destabilizing. Acts of war may justify an offensive response, but conventional or nuclear deterrence is more appropriate when attempting to deter aggression defined by war. Complicating cyberspace deterrence is the lack of attribution, no traditional constraints associated with rational behavior of extremists, and a deficient United States cyber national strategy.

The next chapter of this paper reviews recent United States strategies and critical cyber infrastructure, attribution in the cyber domain, and cyber espionage. Chapter three provides analysis of cyber terrorism and nation-state operations in the cyber domain. Chapter four describes cyber deterrence recommendations aimed at countering terrorists as well as United States peer competitors. The final chapter presents conclusions.

Technologies to attribute actions within the cyber domain are essential if any type of deterrence strategy is to be effective.[4]

Chapter 2

Background

National Security Strategy and Critical Infrastructure

The 2002 United States National Security Strategy (NSS) states, "traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents."[5] Four years later, the 2006 NSS states, "The new strategic environment requires new approaches to deterrence and defense."[6] The current NSS focuses on several "essential tasks" to meet America's national security challenges.[7] Its aim is to promote democracies, prevent terrorist attacks, and support global economic growth. The NSS hardly mentions cyber security, cyber infrastructure, nor does it consider cyberspace a vital national interest.

The United States has become increasingly reliant upon the global cyber infrastructure. The 2006 National Infrastructure Protection Plan (NIPP) states, "protecting the critical infrastructure and key resources of the United States is essential to the Nation's security." It goes on to state, "direct terrorist attacks and natural, man-made, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects."[8] A critical piece of many commercial networks is the command and control system called Supervisory Control and Data Acquisition or SCADA. SCADA systems manage critical infrastructure tasks in support of many industrial processes such as energy production, pressure and flow in pipelines, control of transportation systems, and others.[9]

The NIPP mentions SCADA seven times over 196 pages, but does very little to identify those SCADA systems that would result in national level consequences should a compromise occur. The NIPP does mention the National Asset Data Base (NADB), but this system seems to be of limited value when making decisions concerning national security policy. The NADB contains information on over 77,000 individual assets, ranging from nuclear power plants to petting zoos.[10] The presence of a large number of entries generally associated with the latter and having little national relevance has resulted in criticism from the United States Congress.[11] Equally disturbing is the NADB data submissions are all voluntary.

Security for SCADA is typically five to ten years behind corporate information management systems because of its historically isolated stovepipe structure.[12] Traditionally, computer security activities have focused on the "enterprise" side of the network while paying little attention to the parallel networks associated with SCADA systems. As more and more SCADA systems migrate away from their proprietary protocols running on physically separated networks, the associated process control data migrates to business networks and the Internet.

Recent events in the summer of 2008 demonstrate nuclear power plant networks may be vulnerable to cyber-based incidents. At a nuclear power plant in Georgia, a software update and subsequent reboot to a computer operating on the plants business network resulted in plant shutdown.[13] A more serious incident occurred at an inactive nuclear power plant in Ohio were computers became infected by the Slammer worm in January 2003.[14] The worm entered the plant through an unsecure contractor network that bypassed the plant's firewall.[15] Plant engineers had failed to install a 6-month old Microsoft patch.

Each of these incidents demonstrates the increasing connectivity between SCADA systems and corporate business networks resulting in SCADA access from the Internet. This

should be of concern to security professionals entrusted with maintaining these systems due to a changing threat environment. During the period from 1982 to 2000, insider employees committed approximately 70 percent of cyber incidents. From 2001 to 2003, the pattern reversed to 70 percent of computer security incidents originating externally.[16] These numbers continue to climb as more companies see security breaches originate from Internet connected sources.[17]

Vulnerabilities do exist in America's energy infrastructure, and as more SCADA networks connect to the Internet and more applications rely on Microsoft products, these vulnerabilities may increase rather than decrease. National strategy to address these changes in critical infrastructure and the associated threat is significantly lacking in United States security strategy documents. The most disturbing scenario some envision is the possibility of a parallel strategy using cyber-attacks on critical infrastructure in conjunction with physical attacks.[18] However, without attribution in the cyber domain, linking a cyber-attack to a terrorist group or government is difficult at best.

The Problem of Attribution

A critical requirement for effective cyber deterrence is the concept of attribution. The United States Air Force defines attribution as "the process by which one can ascribe an attack to a particular person or organization."[19] Computer operations traversing the Internet are inherently anonymous because the underlying infrastructure and protocols do not support attribution. As a result, identifying the source of a cyber-attack is nearly impossible when an attacker uses the common techniques associated with many of today's distributed denial of service (DDoS) attacks. DDoS attacks typically involve an assailant using a compromised computer to launch attacks against and through other machines across a network.[20] Packet trace-back techniques offer one possible solution to identify the source of an attack through one or multiple networks.

Some network equipment manufacturers such as Cisco are now offering software tools that will trace traffic from a denial of service attack back to its source.[21]

Other tools and methods that attempt to provide a level of attribution include Ingress filtering. This method requires all message traffic entering a network to have a valid Internet Protocol (IP) source address belonging to the known set of IP addresses in the originating network.[22] Obviously, this method would significantly decrease IP address spoofing, provided it were implemented by a majority of the world's Internet service providers (ISP). Still other tools include honeypots and honeytokens. A honeypot is a decoy system, while a honeytoken is decoy information. The problem with each of these examples is that they are unable to distinguish between malicious attackers and unknowing compromised users.

There is a significant difference between identifying a cyber-attack source, and linking the attack to a human or government. Cyber-attackers ensure their anonymity by utilizing IP spoofing, media access control spoofing, or employment of large botnet armies. Botnets consist of hundreds or thousands of compromised computers routinely used to accomplish DDoS attacks or harvest information.[23] Attribution in this environment will be difficult to accomplish.

Privacy and Attribution

The notion of attribution conflicts with many current privacy policies due to the information required for successful attribution can be very sensitive and requires protection against unauthorized access. Congress enacted the Federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) in an attempt to balance individuals right to privacy and the legitimate needs of law enforcement.[24] Section 2511 prohibits the interception and disclosure of wire, oral, or electronic communications without a specific court order.

Important exceptions to the Federal Wiretap Act law exist in relation to an ISP. For example, it is legal for a service provider "to intercept, disclose, or use communications in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service."[25] However, prior to enactment of the United States Patriot Act, it was illegal for law enforcement agents to identify a hacker who had illegally penetrated a government computer, as well as most domestic computer systems, without first obtaining consent or a court order.[26] The Patriot Act implemented two important changes:

- Established a new exception for intercepting communications of "computer trespassers,"
- Directed sharing of information between law enforcement and intelligence agencies.[27]

The Patriot Act goes on to define a computer trespasser as "a person who accesses a protected computer without authorization and thus, has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer."[28]

Balancing privacy with security is an important consideration when dealing with the issue of attribution. In August of 2004, President Bush signed Homeland Security Presidential Directive-12 (HSPD-12). HSPD-12 created a requirement for "secure and reliable" identification of all Federal government employees and contractors.[29] In February 2005, the Department of Commerce's National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) 201, commonly referred to as FIPS-201. A key element of FIPS-201 is employee privacy protection. Unfortunately, the Federal government has been slow to fully implement HSPD-12 and take advantage of FIPS-201. As of October 2008, only 29 percent of federal employees and contractors held the new FIPS-201 compliant smart cards.[30]

Federal initiatives provide important tools that protect both the cyber domain and personal privacy; however, the task of attributing unauthorized cyber activity and ultimately deterring unwanted cyber behavior will continue to require additional research. Also important will be updates to future domestic and international law.

Espionage versus Cyber-attack

It is important to distinguish between cyber espionage and cyber-attacks. Espionage is traditionally thought of as spying, a very different concept when compared to the use of force. The United Nations (UN) Charter of 1945 makes an important distinction between espionage and use of force.

Article 2(4) of the UN Charter places certain prohibitions on the use of force and states, "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[31] As a result, there has been a long-standing acceptance of espionage as a legitimate action under Article 2(4). However, this Charter was drafted at a time when major wars, to include nuclear war, were perceived as the most probable conflicts of the time. In the cyber domain, an act of espionage can be committed from outside the nation-state victim, making prosecution reliant on extradition. However, under international law, there is no right to extradition,[32] and therefore, no nation is likely to extradite an agent who commits cyber espionage.[33] Today, the UN Charter has trouble adjusting to an era of terrorists and nation-states conducting operations in the cyber domain.

The difference between cyber espionage and cyber-attack is important because cyber espionage provides an opportunity for successful, repetitive intelligence gathering, through the manipulation of software. During cyber espionage, an agent may leave a trap door behind resulting in countless acts of espionage, a far different incident when compared to traditional

physical espionage.[34] International law permits cyber espionage in much the same way as traditional espionage; however, it is typically a crime under domestic law.

Destruction with real world physical results defines cyber-attack.[35] Scope, intensity, and duration identify the significance of a cyber-attack.[36] However, most cyber-attacks seen to date do not rise to a level that allows for use of force as defined by the UN Charter. Perhaps deterrence of cyber-attacks and cyber espionage is possible with a strong network defense strategy, in much the same way physical security barriers may deter physical attacks and traditional espionage. This makes sense as the international community attempts to define appropriate legal measures to address the cyber domain.

There are no easy answers. The deterrence of state sponsors is a start, but so, too, must we find ways to delegitimize the idea and subvert the movement. That notion has been at the heart of the counterinsurgency strategy that we have employed in Iraq: replace the fear that terrorists hope to engender with the very hope they fear to encounter.[37]

Chapter 3

Analysis

Cyber Terrorism: Does it Exist?

Debate on America's vulnerability to cyberspace threats has received increased attention recently. Vulnerabilities continue to multiply as the United States economy becomes more reliant on the Internet, government and private sectors continue to report cyber penetrations, and SCADA systems controlling the nation's critical infrastructure turn out to be nothing more than computers and servers running Microsoft's legacy operating systems.

Since the attack of September 11, 2001, published literature focused on the looming cyber terrorism threat has seen a significant increase. In April 2003, Tom Ridge, then Director of Homeland Security stated, "Terrorists can sit at one computer connected to one network and create worldwide havoc."[38] In 2003, a survey of 725 cities conducted by the National League of Cities ranked cyber terrorism as a top "fear" for the majority of city officials.[39] Recent research suggests there are upwards of 5,600 web sites that promote al-Qaeda ideology and this number is growing by 900 new sites every year.[40] However, real cyber-attacks that result in death and mayhem remain the rhetoric of alarmists and profiteers.

Terrorist Tactics and the Internet

A recent Government Accountability Office (GAO) report states, "terrorist adversaries of the United States are less developed in their computer network capabilities than other

adversaries."[41] Terrorists likely pose a limited cyber threat to the United States given their minimal sophistication in conducting cyber-attack operations. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks."[42]

Current estimates show over 41 million Internet users in the Middle East, with an impressive usage growth rate of 1,176 percent from 2000 to 2008.[43] Even remote Afghanistan, with a population of over 32 million has an estimated 600,000 Internet users, a sizeable increase from only 1,000 users in 2000 when Internet usage was banned under Taliban rule.[44] With Internet usage on the rise in the Middle East, and terrorists operating freely in the cyber domain, American cyber deterrence strategy should focus on terrorist activities and values.

Terrorism is not about terror. However, terrorists use the global information infrastructure in many ways to support their ideological ends. Terrorists find Internet usage attractive because it is cheaper, more anonymous, offers more targets, and provides the ability to reach a larger number of people.[45] The terrorist center of gravity (COG) is their popular support both in the local and international populations. The Internet is the medium used by terrorists to reach their COG. Because the terrorist COG resides in the cyber domain, it is here that deterrence must operate.

Terrorists hold a decided edge in the information domain. Terrorists use the Internet for propaganda dissemination, recruitment, communications, fund raising, and operational execution.[46] Terrorists routinely present their propaganda to supporters in the local language with detailed information concerning their cause and activities. They will target the international public through press releases and historical background information in a variety of languages. Engagement of terrorists through the cyber domain is required if local populations around the

world are to renounce violence and embrace the legitimacy of counterterrorism efforts. At the opposite end of the threat spectrum is cyber usage by peer competitors of the United States.

Nation State Peer Competitors

Nations such as China and Russia seek to improve their ability to operate in the cyber domain for a variety of reasons to include exploitation of the United States information infrastructure, potential disruption or destruction of information infrastructures during some future conflict, and for intelligence collection.[47] The range of threats includes malware, phishing exploits, network penetrations, and botnets to name just a few. The difficulties associated with attribution hinders the United State's ability to clearly identifying foreign government sponsored activates versus criminal or hacker actions. However, what may be most disturbing and is least understood by Western analysts is China's expansion from the traditional air, land, and sea battlefield domains to the space and cyber domain.

The Chinese continue to base their military strategy on the writings of Mao Tse-tung. China's vision is one of a People's War, the mobilization of the entire population in a struggle for the motherland. Taking this vision into the cyber domain presents the possible relationship between the People's Liberation Army (PLA) and Chinese hacker organizations. One example is the "Red Hacker Alliance."[48]

Research has shown many of the recent cyber-attacks that trace back to China in fact originated within the Red Hacker Alliance. Its membership has grown from a few thousand to over 300,000, mostly young male nationalists.[49] China denies any relationship with the Red Hacker Alliance, claiming Chinese law forbids attacks using the Internet.[50] Denying association while tolerating Red Hacker Alliance operations provides China with plausible deniability.[51]

It is doubtful the Chinese government actually accounts for so many cyber-attacks as the PLA would not be so injudicious as to attempt intrusions from easily indefinable government accounts.[52] One possibility is that a lack of computer systems security updates and heavy reliance on pirated software has resulted in China becoming a haven for botnet command and control sites (C2).[53] In either case, the existence of the Red Hacker Alliance demonstrates a significant expansion of Chinese civilian actions focused on cyber-attack and cyber operations. This drives cyber deterrence towards a strong defensive posture versus offense actions against the civilian population of a peer competitor like China.

Cyber defense is required when considering China has downloaded approximately 10 to 20 terabytes of data from the Department of Defense's (DOD) Non-classified Internet Protocol Router Network (NIPRNET) looking for opportunities to comprise military personnel identities and passwords in order to gain access to other DOD networks.[54] Moreover, although some American government circles downplay this compromise because no classified information is involved, the NIPRNET does provide the primary infrastructure for a majority of DOD's logistics and transportation scheduling, not to mention the majority of human resource databases related to military and government civilian personnel.

China's military thinkers routinely write on information warfare, and demonstrate knowledge of the United States military's dependence upon information. For example, a November 2006 *Liberation Army Daily* commentator argued: "The mechanism to get the upper hand of the enemy in a war under conditions of informatization finds prominent expression in whether or not we are capable of using various means to obtain information and of ensuring the effective circulation of information and, whether or not we are capable of applying effective

means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment."[55]

The 2007 Annual Report to Congress on *Military Power of the People's Republic of China* reports the PLA is transforming its large ground-based army to one ready to fight "short-duration, high-intensity conflicts against high-tech adversaries," which China defines as "local wars under conditions of informatization."[56] The report goes on to state, "The PLA has established information warfare units to develop viruses to attack enemy computer systems. In 2005, the PLA began to incorporate offensive computer network operations into its exercises, primarily in first strikes against enemy networks."[57]

The recent Russian conflict in Georgia demonstrates a cyber first strike principle in real world operations. In July 2008, probes of Georgian web sites and other computer systems began. The Russian press reported a DDoS attack aimed at the South Ossetia government just hours before initiation of military hostilities.[58] Analysis of the cyber assault upon Georgia is surprisingly inline with Russia's military efforts. A recent report on the emerging global cyber threats demonstrates how Russian attacks and timing align:

- DDoS traffic logs and modifications in network routing indicate cyber warfare operations aligned with the initial Russian Air Force attacks,
- Cyber targets and air force targets were both located in the city of Gori,
- Updated cyber targets and subsequent Russian Air Force attacks in Gori implied coordination between the Russian military and known hacking groups.[59]

The main similarity between Russian and Chinese cyber warfare programs appears to be an offensive doctrine emphasizing a "first strike" mentality.[60] Russian cyber doctrine states, "enemy access to external information should be denied, credit and monetary circulation should

be disrupted, and the populace should be subjected to a massive psychological operation--including disinformation and propaganda."[61] This doctrine appears to be inline with the cyber-attacks against Georgia.

Given China's focus on information warfare, and even the remote possibility of Russia's coordinated cyber-attacks against Georgia, United States efforts to deter foreign preparation for these types of parallel attacks against American national interests would be appropriate.

We need a new model for deterrence theory, and we need it now. Time is not on our side. Traditional concepts of deterrence will not work against a terrorist whose avowed tactics are wanton destruction and the targeting of innocents.[62]

Chapter 4

Recommendations

Cyber Deterrence of Terrorism

It should be clear deterrence during the Cold War was more straightforward than deterrence of today's terrorist. Terrorists do not have cities, industry, or military bases to strike as a deterrent response. Threatening punishment of terrorists does little to persuade those who support violent extremism. However, by operating in the cyber domain and focusing on terrorist ideology and goals, perhaps tailored deterrent options can emerge to counter global terrorism.

As mentioned before, terrorists use the Internet for propaganda, recruitment, communications, fund raising, and operational execution. Deterrence of terrorist activities such as propaganda distribution and recruitment requires a robust cyber-based virtual diplomacy effort. This is no trivial task in the international arena. It will require close cooperation across the United States interagency process to ensure the translation of communications into influence through a thorough understanding of language, culture, and values of the target audience.[63]

An important first step in countering terrorist propaganda and recruitment efforts would be the creation of regional strategic communications plans. The plans would define core messages, segment target audiences, identify goals, and analyze measures to evaluate results.[64] Core messages should focus on the presentation of facts to include United States goals and policy for Iraq and Afghanistan, as well as success stories associated with Provisional Reconstruction Teams (PRT) or the United States Agency for International Development

(USAID). Segmentation of target audiences would require input from United States Embassies to tailor messages for individual countries or tribes. Goals must be set for research efforts to uncover rumors or terrorist propaganda quickly and then accurately respond. Finally, defined measures of success are required, for example, reduced "negative" rumors or a reduction in terrorist propaganda. Success stories should promote the local population's efforts and their linkage to PRT or USAID projects. In this way, downplay of American efforts allows host-nation achievements to build credibility and encourage confidence from the local target audience.[65] Any regional strategic communications plan must take into consideration the need to coordinate efforts across diplomatic and military channels. Coordination is critical to any terrorist deterrent effort to ensure synchronization of actions and promises, because facts will speak louder than words.[66]

Communications in the 21st century have evolved into new collaborative forums such as on-line communities of interest, public web hosting, blogs, and streaming video. Terrorists have embraced these communications tools because they are swift and allow dispersed leaders to communicate with the masses. These tools are also inexpensive and provide for easily shared information. One way to deter the usage of Internet communications tools is to identify terrorist sponsored web sites, and shut them down. Publicly identifying and then encouraging the ISP to turn off service to the terrorist web site may be one option, provided this type of shaming can influence the provider. The downside to this option is once a terrorist web site is non-operational it removes an important venue to analyze terrorist activities and plans. Other options include deployment of credible communications tools like blogs or on-line news coverage led by the local indigenous population with content designed by the same.

Foreign countries typically view information published by the United States government as self-serving and inconsistent. Consensus among youth in the Muslim world is that Americans stereotype all Muslims as terrorists.[67] Add to this Abu Ghraib and Guantanamo, and it becomes easy to understand why those living in foreign lands view United States policy as anti-Muslim.

Efforts in London and Singapore demonstrate how leaders can encourage an anti-extremist message from within the local population and then use the Internet to communicate the message. Following the London bombings, 500 British Muslim leaders condemned the perpetrators with a religious decree.[68] The British government sponsored a Muslim task force that recommended the presentation of a mainstream interpretation of Islam to young British Muslims. As part of this effort, the organization called Radical Middle Way (RMW) was established. The RMW web site states its purpose is to reject terrorism, revive public service, and encourage a sound British Muslim identity.[69] In Singapore, leaders have adopted a program sponsored by the Religious Rehabilitation Group (RRG), a group of 30 Muslim clerics who voluntarily assist in illustrating to terrorist detainees and their families that a violent interpretation of Islam is wrong.[70] The difficulty for American efforts to embrace these initiatives as deterrence options is the possibility of tainting the message through an appearance of American sponsorship.

The United States has made efforts to improve its image throughout the Middle East by supporting regional broadcasters to include Radio Sawa and Al-Hurrah satellite television; however, garnering support from the mainstream Muslim world is the key requirement.[71] The communications goal should be to discredit violent extremism. This message gains credence when content and media distribution occur from within the local indigenous population. Islamic scholars and clerics are highly influential and as such, the United States should promote those

who reject violence and terrorist acts.[72] Reformed terrorists offer an additional source for communicating an anti-extremist message.[73] Celebrity figures who promote mainstream messages of peace can influence the local population provided there is a strong celebrity following in the target community.[74] The goal in each example is to provide a mainstream voice to the anti-extremism message. Successfully discrediting violent extremism may also dissuade local populations from providing financial support to terrorist organizations.

Terrorists use the Internet to raise funds by encouraging believers to make on-line donations. Typically, a terrorist web site will provide banking information and account numbers for direct deposit of donations.[75] Some web sites even provide information for credit card deposits.[76] Deterrence of this type of terrorist support is possible when the local populace receives credible anti-terrorist messages from local figures. Domestically, strengthening United States laws to counter terrorist fund raising provides a means of deterrence. Passage of the Patriot Act strengthened domestic legal measures to combat terrorist financing. Title 18 of the United States Code defines federal crimes associated with financing terrorism to include providing material support for terrorist offenses or to foreign terrorist organizations, providing or collecting terrorist funds, and concealing funds used for terrorist acts.[77] As of August 2005, the United States had frozen over $281 million in terrorist related funds, including over $264 million of related Taliban funds.[78] Although significant legal measures are in-place to address terrorist funding, the low cost of entry to the cyber domain reduces the effectiveness of financial penalties to deter terrorist activities.

Perhaps the most difficult deterrence option is the attempt to dissuade actual planned terrorist operations. Terrorist groups routinely use chat rooms and email to coordinate activities across the globe. Distribution of instructions occurs with maps, text directions, and details for

such tasks as bomb assembly, all typically concealed using steganography. Instructions may also be disguised using simple coded phrases. The last message from Mohammed Atta to the other 9/11 terrorists reportedly read, "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering."[79] Hindsight reveals Atta's references to faculties being a coded message linking the number of confirmed terrorists to the four buildings targeted for attack. The study of email traffic, chat sessions, or text posting to terrorist web sites may provide leads to terrorist targets, timing, or scope of a planned operation.

Deterring terrorists from carrying out planned attacks is also possible with sound intelligence gathering and effective law enforcement to confirm terrorist planning efforts. Deterrence may focus on increased security at the target, which was the case in the 2003 al-Qaeda plot to bomb the Brooklyn Bridge, or public disclosure of planned operations and subsequent arrest of suspects to signal terrorists that their plans have been unveiled. Estimates indicate the disruption of at least 19 terrorist plots against the United States since 9/11.[80]

By improving on-line "deception" detection, surveillance of known terrorist web sites may result in identification of additional terrorist plans prior to execution. Research at the University of Arizona is focused on just such technology. A model for human behavior associated with deceptive intentions may result from analyzing language, voice, and video gestures.[81] The model could provide a critical tool to deter terrorist usage of the Internet in planning and executing extremist attacks.

Peer Competitors and Cyber Deterrence

The 2006 NSS states East and Southeast Asia's "stability and prosperity depend on our sustained engagement: maintaining robust partnerships supported by a forward defense posture

supporting economic integration through expanded trade while promoting democracy and human rights."[82] It goes on to state, "The United States seeks to work closely with Russia on strategic issues of common interest and to manage issues on which we have differing interests.[83] Clearly, America seeks stability, mutual collaboration, and partnerships with China and Russia. Direct confrontation between the United States and China or Russia is not likely; however, involvement of either of these major powers in a regional confrontation, such as the recent Georgian confrontation, remains a legitimate possibility.

A regional confrontation with China may very well involve Taiwan. Taiwan has emerged as a global supplier of information technology and computer components. Dell and Hewlett-Packard spend billions of dollars on computer parts manufactured in Taiwan.[84] Taiwan is currently the largest manufacturer of computer components, and some call it "a hidden center of the global economy," acting as a go-between for American computer makers and Chinese assembly plants.[85]

Similar too many American reports of domestic computer attacks originating in China, Taiwanese government computers are attacked approximately 99 percent of the time from IP addresses in China.[86] Any cyber-scenario involving a Chinese regional conflict with Taiwan would more than likely mirror Estonia or Georgia, where China would seek to degrade cyber infrastructure, command and control networks, and possibly financial or media cyber capabilities in a preemptive first strike assault. However, current Chinese strategy does look to downplay its capabilities and avoid confrontation over Taiwan.[87] Nevertheless, the stakes are high when it comes to China's position on Taiwan, while the lack of attribution associated with a Chinese initiated cyber-attack make cyber deterrence of a regional power like China difficult.

Given this type of scenario, and the low probability of direct confrontation between China and the United States, cyber deterrent options should focus on engagement with regional partners through diplomatic and financial channels with the goal of integrating China into the international community.

Diplomatic and Economic Engagement as a Cyber Deterrent Option

The United States engagement policy towards China seeks to avoid conflict. Deterrence should not be the defining criterion to United States-China relations. Continued efforts that provide China incentives to maintain good relations with the United States are the best course of action. Therefore, any cyber deterrence option requires careful analysis so as not to disrupt United States-China relations.

Chinese leaders are concerned with regional security issues. They seek to maintain stability along Chinese borders while advancing strategic economic and political interests throughout Asia.[88] China perceives an independent Taiwan as a threat to Chinese legitimacy of such magnitude that moves in such a direction could result in the over-throw of China's leaders.[89] Taiwan's strength comes from its economic influence and ties with the United States.

Taiwan's gross domestic product is larger than any member of the Association of Southern Asian Nations (ASEAN).[90] The United States most important trade partner when it comes to information technology is Taiwan. United States trade relations with Taiwan are a condition of diplomatic relations between the United States and China, and reinforced by the Taiwan Relations Act (TRA). As of December 2000, the United States and Taiwan established approximately 98 international agreements under TRA guidelines.[91]

Although China views increasing friendly relations between America and Taiwan as an irritant, if traditional trading partners see the United States migrating away from the region due

to pressure from Beijing, other regional allies may question their relationship with the United States. To deter Chinese exploitation of the cyber domain, America would be wise to look for opportunities to strengthen trade opportunities tied to cyber security, especially with Taiwan given its huge information technology export industry. The United States should also continue efforts to collaborate on cyber defense strategies with various ASEAN countries and Taiwan.

Some initial dialog has occurred that supports collective cyber defense strategies in Southeast Asia. The ASEAN Regional Forum (ARF) is a security cooperation forum comprised of 28 participants to include the United States, China, Russia, and the European Union. ARF members are working towards an alert network to facilitate threat and vulnerability notification along with distribution of software patches.[92] In October 2007, the 4th ARF Seminar on Cyber Terrorism facilitated the exchange of information and ideas concerning the rise of cyber terrorism in the region. Topics discussed covered a range of cyber issues to include "Cooperation on Cyber Security within the ARF." Unfortunately, the ARF is not a collective defense organization, nor does it provide a mechanism for collective security. The ARF tends to facilitate dialog among member states to enhance confidence across the ARF while focusing on preventive diplomacy rather than deterrence.[93] The ARF does offer a mechanism to resolve disagreements in order to avoid conflict. It also offers a starting point from which the United States may engage Southeast Asian countries on the subject of collective cyber defense.

When considering some future possibility of China launching a parallel physical and cyber-attack in a regional confrontation, the United States must be concerned with increased outsourcing of commercial software by American firms to foreign countries. Some argue "offshore outsourcing" is the most serious threat to the United States software industry."[94] This raises the question of possible imbedded vulnerabilities in both hardware and software developed

by foreign information technology manufactures. Oracle, a major supplier to American intelligence agencies, has in the past, outsourced software development projects to China.[95] This issue does offer some minimal deterrence options from an economic engagement position.

Future trade agreements and contracts should consider standards that ensure computer security for new systems and provide methods to ensure certification. Contracts must ensure physical security of manufacturing areas and assembly areas. Formal agreements should also provide for on-site monitoring of plants. Considering the significant global concern for secure computing, this should be a feasible task in any future trade agreements or contracts involving ASEAN countries or firms.

Cyber Defense, More than Passwords

At the heart of deterrence lies credibility. With the lack of adequate attribution in the cyber domain, regular demonstration of cyber defense capabilities could be a convincing deterrent. Unfortunately, the DOD and a significant portion of the Federal government have had limited success in defense against cyber-attacks. A review of the 2007 Federal Information Security Management Act (FISMA) report card on computer security shows an overall grade of "C-minus" for Federal Departments and Agencies and for the second year in a row, the DOD grade was an "F." In addition, the recent banning of all removable thumb drives from DOD networks in response to an Internet worm[96] is hardly a successful demonstration of sound cyber defense. Instead, this lack of resiliency does little to deter future malware attacks, and instead sends a signal the United States military is unprepared for a cyber-attack. Much more is required to deter the types of attacks seen in Estonia and Georgia. In order for the United States to present at least a modicum of credibility in its attempt to secure cyberspace, it must look at renewed

emphasis on information assurance (IA), support for strong authentication to critical infrastructure, and investment in secure cyber infrastructure.

Private industry and the DOD both advocate a strong defense in depth strategy for IA. United States military guidance requires a robust defense in depth strategy to anticipate and preempt adversary cyber-attacks while minimizing effects, reconstituting the network, and preventing reoccurrence.[97] Simply stated, defense in depth employs layered barriers between an attacker and critical information systems. However, it is important to note this strategy is a process, not a technical solution. Therefore, it should employ a protect, detect, and react paradigm.[98]

Well-configured firewalls offer one method of protecting critical information systems. Firewall configuration must only allow port and protocol traffic necessary for mission accomplishment. The firewall rule set must be fully documented, and reviewed on a routine basis for necessity.[99] However, firewall management is far from trivial, and requires highly trained and skilled IA professionals. Equally important is network monitoring to detect intrusions. Intrusion detection systems (IDS) provide the preferred method for network monitoring. Pre-defined rules and attack "signatures" allow the IDS to monitor network traffic for abnormal activities and then execute pre-determined instructions.[100]

Perhaps the most important aspect of a defense in depth strategy is security policy and training to enable the proper reaction by personnel. In the DOD, this is particularly important when dealing with the Secure Internet Protocol Router Network (SIPRNET). The Defense Information Systems Agency (DISA) compares the SIPRNET to candy, a hard outer shell with a soft center.[101] The physical security around the SIPRNET and its infrastructure is sound, but if

the boundary is breached this could lead to a breach of the network.[102] Some of the DOD C2 systems are legacy and utilize outdated versions of the Windows operating systems. Therefore, military C2 systems are more susceptible to malware, and because of their complex nature may be more time-consuming to recover from such a mistake. Just as disturbing is the possibility of an inside user accidentally introducing a virus or other malware to the SIPRNET.

User training is critically important when it comes to security. Threats can come from phishing scams, spyware, weak passwords, or other malware. Users may introduce threats to the network by responding to phishing scams, or by bringing infected removable media from home and introducing it to a DOD network. A robust user-training program, regular exercises to test user knowledge and response, and clearly defined consequences for failure to follow approved security policy are critical to protection of DOD networks. Just as important as user training is the issue of user authentication.

The Interagency Working Group (IWG) on Cyber Security and Information Assurance (CSIA), an organization under the National Science and Technology Council (NSTC), recently surveyed federal agencies to determine their cyber research and development priorities. The one item consistently identified as a top funding priority for cyber security was authentication.[103]

The DOD currently uses smart cards with public key infrastructure (PKI) technology as a means to access the NIPRNET. PKI technology provides multiple security capabilities to include assured electronic transactions, digital signatures, and encrypted unclassified messages. Intrusion into DOD networks has dropped by over 50 percent following the deployment of Common Access Cards (CAC).[104] Usage of stronger authentication such as PKI and FIPS-201 compliant smart cards for access to critical infrastructure like SCADA or SIPRNET could significantly deter future intrusion attempts by experienced attackers. However, key to smart

card success has been PKI, which is reliant upon investment in an infrastructure built to provide third party issuance of trusted certificates.

A strong cyber investment strategy must focus upon secure protocols and infrastructure. Federal acquisition efforts should lead the way in acquiring secure products by focusing cyber efforts on secure Internet protocols. Many Internet Relay Chat (IRC) tools transmit passwords unencrypted across networks. The File Transfer Protocol (FTP) exchanges both data and login information unencrypted. FTP is one of the most widely used protocols for Internet file transfer, and commonly seen in both federal government and military computer systems. Cyber investment must move beyond quarterly purchases of computers loaded with the latest Microsoft operating system towards a strategy focused on network security in the design process, rather than simply assuming physical security during systems deployment. Only then will the deterrent value of demonstrated cyber security and investment prevail.

The ability to mount a credible cyber defense against potential cyber-attackers can be in itself a plausible cyber deterrent. The United States government and the DOD have displayed limited success in preventing cyber-attacks. What is required to deter nation-state competitors from continuing routine probes and attacks upon the DOD and United States cyber infrastructure is a renewed emphasis on IA, network authentication, and investment in a secure cyber infrastructure.

Chapter 5

Conclusion

Traditional Cold War deterrence models will not work in the cyber domain. The threat of cyber-attack is a new paradigm that is potentially dangerous in new and different ways to the global cyber infrastructure. A lack of attribution makes deterrence in this environment difficult and highly unlikely. A new way of looking at deterrence in the cyber domain is required.

The Internet provides an asymmetrical battlefield comparable to what terrorists enjoy in the physical world, the ability to choose the time and place for attack based on exploitation of a few vulnerabilities.[105] Unlike terrorists, nation-states like China have different strategic goals and therefore each require different strategies and options for deterrence.

Terrorists use the cyber domain for propaganda, resources, and operational communications. Even if attribution existed in the cyber domain, this may not deter extremist organizations as many times terrorist groups seek to affirm their responsibility for terror attacks to gain benefits from the associated propaganda. What may deter terrorist's cyber domain usage and ultimately dissuade their extremist actions is the perception that they will be unable to accomplish their goals. Regional based strategic communications coordinated across the federal government and focused on host-nation success stories is a sound starting point.

A coordinated effort that integrates both diplomatic and military instruments of power is required. Efforts such as British based Muslim leaders condemning violence and Singapore's efforts at rehabilitation of terrorists warrant support. Defeating terrorists in the cyber domain means destroying terrorist messages and propaganda used to recruit and build support from local populations. Support of mainstream Muslims such as Islamic clerics, reformed terrorists, and

celebrity figures ensures legitimacy of a mainstream message that rejects terrorism. In addition, careful study of known terrorist web sites and development of new methods to analyze information can help deter terrorists from carrying out their plans. Deterrence of terrorists in the cyber domain requires consideration of a wide range of options that address how terrorists use the Internet and what their goals entail.

Russia and China have embraced the cyber domain with doctrine that supports a "first strike" mentality. Coupled with an understanding of the United State's heavy reliance on command and control through networked operations, parallel physical and cyber-attack is the most likely threat. The United States government's poor cyber security and increasing reliance on the Internet by SCADA systems provide ample targets for nation-states to attack America's cyber infrastructure. The lack of attribution and limited definitions for illegal cyber activity make a strong cyber defense the best cyber deterrent option to address peer competitors. The United States should focus efforts on cyber security, network authentication, and cyber investment.

Lastly, because the United States desires good relations with China, America should continue efforts to provide China with incentives to become a strong supporter of the global community. Engagement through regional organizations such as the ASEAN Regional Forum and future trade agreements that ensure security for imbedded computer systems can help deter introduction of security vulnerabilities by foreign information technology manufactures.

Although these options may be difficult to implement, the United States cannot rely on traditional Cold War deterrence methods in the cyber domain. Deterrence in a multi-polar world must incorporate new thinking and threat based analysis to have any chance of success.

Bibliography

Adams, Charlotte. "Securing Information Vexes Defense Planners." *Signal Magazine*, vol. 63 no. 3 (November 2008): 103-107.

al-Faram, Khaled. "Researcher: Al-Qaida-linked Web sites number 5,600." ZDNet News, 4 December 2007. http://news.zdnet.com/2100-9588_22-178795.html (accessed 17 December 2008).

Ali, Mohamed Bin. *De-Radicalisation Programmes: Changing Minds*? RSIS Commentary No. 100, 23 September 2008.

Annual Report to Congress. *Military Power of the People's Republic of China 2007*.

Bassett, Richard, Vincent Ierace, Ellen Murphy, and Riccardo Palmerini. "Security Risks Associated with Geosourcing." *The ISSA Journa.* (September 2004): 22-27.

Billo, Charles, and Welton Chang. *Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States*, Hanover, NH: Institute for Security Technology Studies, Dartmouth College. Revised December 2004.

Blumenthal, Dan, and Randall Schriver. "Strengthening Freedom in Asia, A Twenty-First-Century Agenda for the U.S.-Taiwan Partnership." Washington DC**:** The American Enterprise Institute, 22 February 2008.

Byres, Eric, and Justin Lowe. *The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems.* Technical Support Working Group. Washington DC: 4 October 2004.

Carafano, James Jay. "U.S. Thwarts 19 Terrorist Attacks Against America Since 9/11," *Backgrounder*, no. 2085. Washington DC: The Heritage Foundation, 13 November 2007. http://www.heritage.org/research/HomelandDefense/bg2085.cfm#_ftn20 (accessed on 17 December 2008).

Charter of the United Nations: Article 2(4), June 26, 1945. http://www.yale.edu/lawweb/avalon/un/unchart.htm#art2 (accessed on 1 February 2009).

Correspondents in Kuala Lumpur. "Region hatches cyber defence." *Australian IT*, 31 July 2006. http://www.australianit.news.com.au/story/0,24897,19966914-15331,00.html, (accessed on16 January 2009).

Dacey, Robert F. Statement on *GAO Critical Infrastructure Protection: Challenges in Securing Control Systems: Testimony before the Subcommittee on Technology, Information Policy,*

Intergovernmental Relations, and the Census, House Committee on Government Reform. Report Number GAO-04-140T. Washington, DC: 1 October 2003.

Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. National Security Agency/Central Security Service. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed on 07 February 2008).

Department of Homeland Security, Control Systems Cyber Security: Defense in Depth Strategies. External Report # INL/EXT-06-11478. Idaho National Laboratory, May 2006.

Department of Homeland Security. 2006 National Infrastructure Protection Plan.

Emerging Cyber Threats Report for 2009. *Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond.* Georgia Tech Information Security Center, October 15, 2008., http://gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (accessed on 17 December 2008).

Epstein, Keith. "U.S. Is Losing Global Cyberwar, Commission Says," *Businessweek*, 7 December 2008. http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db2008127_817606.htm (accessed on 17 December 2008).

Field Manual (FM) 3-24. "Counterinsurgency." Washington, DC: Depart. of the Army, 2006.

Ford, Jess T. Statement before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee on Appropriations. *U.S. Public Diplomacy, State Department Efforts Lack Certain Communication Elements and Face Persistent Challenges.* Report number GAO-06-707T. Washington, DC: 3 May 2006.

Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower. 12th ICCRTS Adapting C2 to the 21st Century, Track: C2 Concepts, Theory, and Policy.

Freedman, Lawrence. *Deterrence.* Cambridge UK: Polity Press, 2004.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law.* Washington DC: National Defense University Press, 1998.

Henderson, Scott. "Beijing's Rising Hacker Stars, How Does Mother China React?" *IO Sphere*, (Fall 2008): 23-28.

Higgins, Kelly Jackson. "Taiwan Says China Accounts For Most Cyber Attacks, Information Week." 17 January 2008. http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=208803769 (accessed on 1 December 2008).

Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. *Role and Challenges for Sufficient Cyber-Attack Attribution.* grant no. 2003-TK-TX-0003. U.S. Dept. of Homeland Security. Science and Technology Directorate, January 2008.

Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. United States Code. Title 18, Part I, Ch 119, Sec 2511, para. (2)(a)(i). http://www4.law.cornell.edu/uscode/18/2511.html (accessed 17 December 2008).

IP Source Tracker. San Jose, CA: Cisco Systems, 2008. http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ipst.html (accessed on 17 December 2008).

Kramer, Frank, Stuart Starr, Larry Wentz, Eli Zimet, and Daniel Kuehl.

Krebs, Brian, Cyber Incident Blamed for Nuclear Power Plant Shutdown, *Washington Post*, 5 June 2008., http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html (accessed 17 December 2008).

Lipson, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.* Special Report CMU/SEI-2002-SR-009. Pittsburgh, PA: Carnegie-Mellon ZSoftware Engineering Institute. November 2002.

Lord, Brig Gen William T. *U.S. Air Force Concept of Operations for Information Operations*, 6 February 2004.

McConnell, J. Michael. Statement to House Permanent Select Committee on Intelligence. *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*. Washington, DC: 7 February 2008.

Merriam-Webster Online Dictionary. Springfield, MA: Merriam-Webster, Inc., 2009. http://www.merriam-webster.com/dictionary/deterrence (accessed on 9 February 2009).

Miniwatts Marketing Group. Bogota, Colombia, 1997-2008. http://internetworldstats.com/middle.htm (accessed on 17 December 2008).

Montgomery, Mark C. *Cyber Threats: Developing a National Strategy for Defending Our Cyberspace.* 13 April 2000, repr., Cambridge MA: Program on Information Resources Policy, Harvard University, July 2001.

Moteff, John. *Critical Infrastructure: The National Asset Database*. Report Number RL33648. Congressional Research Service Report for Congress. 16 July 2007.

Mullen, Michael G. "From the Chairman, It's Time for a New Deterrence Model." *Joint Forces Quarterly*, Issue 51, 4th Quarter 2008: 2-3. http://www.ndu.edu/inss/Press/jfq_pages/i51.htm (accessed 1 February 2009).

National Security Strategy of the United States of America. March 2006.

National Security Strategy of the United States of America. September 2002.

Office of Management and Budget. *OMB Reports Significant HSPD-12 Implementation Progress but Areas for Improvement Identified*. OMB Communications, 202-395-7254, Washington DC: Office of Management and Budget, 31 October 2008**.** http://www.whitehouse.gov/omb/pubpress/2008/103108_hspd12.html (accessed 17 December 2008).

Onley, Dawn S., and Patience Wait. *Red storm rising, DOD's efforts to stave off nation-state cyberattacks begin with China.* Government Computer News, 21 August 2006. http://www.gcn.com/print/25_25/41716-1.html (accessed on 17 December 2008).

Ortuoste, Maria Consuelo C. *Reviewing the ASEAN Regional Forum and its Role in Southeast Asian Security.* Asia-Pacific Center for Security Studies. Honolulu, HI: February 2000.

Poulsen,Kevin. "Slammer Worm Crashed Ohio Nuke Plant Net." *The Register*, 20 August 2003. http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/ (accessed 17 December 2008).

Qina, Jialun, Yilu Zhoub, Edna Reidc, Guanpi Laid, and Hsinchun Chen. "Analyzing terror campaigns on the Internet: Technical sophistication, content richness, and Web interactivity." *International Journal of Human-Computer Studies*, 65 (2007): 71-84.

Radical Middle Way, "About Us", www.radicalmiddleway.co.uk (accessed on 17 December 2008).

Religious Rehabilitation Group, www.rrg.sg (accessed on 17 December 2008).

Rollins, John, and Clay Wilson. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Congressional Research Service Report for Congress, updated 22 January 2007.

Sawyer, Ralph D., *Sun Tzu Art of War*. Boulder CO: Westview Press, 1994.

Schmadeka, Roy. "The War of Ideas: The Unheard Voice." *IO Sphere*, (Fall 2008): 6-11.

Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC: Center for Strategic and International Studies. December 2008.

Shea, Dana A. *Critical Infrastructure: Control Systems and the Terrorist Threat*. Report Number RL31534. Congressional Research Service Report for Congress. 20 January 2004.

Shulsky, Abram N. *Deterrence Theory and Chinese Behavior.* Arlington, VA: RAND, Project Air Force, 1999-2003.

Singer, Peter W. "American Goodwill, in Shackles." Washington, DC: Brookings Institution, 26 June 2007. http://www.brookings.edu/opinions/2007/0626islamicworld_singer.aspx (Accessed on 20 January 2009).

Specht, Stephen M, and Ruby B. Lee. *Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures.* Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, September 2004.

Stamp, Jason, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young, "Sustainable Security for Infrastructure SCADA." Report SAND2003-4670C. Albuquerque, NM: Sandia National Laboratories, 2003.

Svan, Jennifer H., and David Allen. "DOD bans the use of removable, flash-type drives on all government computers." *Stars and Stripes,* 21 November 2008. http://www.stripes.com/article.asp?section=104&article=58951 (accessed on 17 December 2008).

Swedlund, Eric. "UA effort sifting Web for terror-threat data." *ARIZONA DAILY STAR*, 24 SEPTEMBER 2007, http://ai.arizona.edu/recognition/uadailystart.pdf (ACCESSED 17 DECEMBER 2008).

Takahashi, Dean. "After the five-day Russia-Georgia war, a chronicle of the cyber battle unfolds." 12 August 2008. http://venturebeat.com/2008/08/12/after-a-five-day-war-a-chronicle-of-the-cyber-battle-unfolds/ (accessed on 17 December 2008).

Tkacik, John J., and Daniella Markheim. "Free Trade with Taiwan Is Long Overdue." *Backgrounder*, no. 2061. Washington, DC: The Heritage Foundation, 15 August 2007.

United States Air Force Scientific Advisory Board. *Report on Implications of Cyber Warfare.* Volume 1: Executive Summary and Annotated Brief, SAB-TR-07-02. Washington DC: HQ USAF/SB, August 2007.

United States Government Accountability Office, Information Security, *TVA Needs to Address Weaknesses in Control Systems and Networks.* Report Number GAO-08-526. Washington, DC: May 2008.

United States: Report on the Observance of Standards and Codes-FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism. IMF Country Report No. 06/432. Washington DC: International Monetary Fund, December 2006.

United States Supreme Court. Dalia v. United States, 441 U.S. 238 (1979). Argued January 9, 10, 1979, Decided April 1, 1979, 441 U.S. 238. *See Dalia*, 441 U.S. at 250 n.9, 252 n.13. http://supreme.justia.com/us/441/238/case.html (accessed 17 December 2008).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001. HR 3162, 107th Cong., 1st sess. Public Law 107-56. October 26, 2001. http://www.fincen.gov/statutes_regs/files/hr3162.pdf (accessed 17 December 2008).

Vasu, Norman. *The London Bombings: Fundamental Change in Fundamentalist Times.* IDSS Commentaries no. 47, 28 July 2005.

Weimann, Gabriel. *Terror on the Internet, The New Arena, the New Challenges*. Washington DC: United States Institute of Peace, 2006.

Weimann, Gabriel. *www.terror.net How Modern Terrorism Uses the Internet.* special report 116. Washington DC: United States Institute of Peace, March 2004.

Wilson, Clay. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.* Report Number RL32114. Congressional Research Service Report for Congress, 17 October 2003.

Wingfield, Thomas C., and James B. Michael. *An Introduction to Legal Aspects of Operations in Cyberspace.* Naval Postgraduate School: Monterey, CA, 28 April 2004.

End Notes

[1] Ralph D. Sawyer, *Sun Tzu Art of War*, (Boulder CO: Westview Press, 1994), 177.

[2] Lawrence Freedman, *Deterrence*, (Cambridge UK: Polity Press, 2004), 7.

[3] *Merriam-Webster Online Dictionary*, (Springfield, MA: Merriam-Webster, Inc., 2009) http://www.merriam-webster.com/dictionary/deterrence (accessed on 9 February 2009).

[4] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare*, Volume 1: Executive Summary and Annotated Brief, SAB-TR-07-02, (Washington DC: HQ USAF/SB, August 2007), 27.

[5] The National Security Strategy of the United States of America, September 2002, 15.

[6] The National Security Strategy of the United States of America, March 2006, 22.

[7] Ibid., 1.

[8] Department of Homeland Security, 2006 National Infrastructure Protection Plan, 1.

[9] Statement of Robert F. Dacey, *GAO Critical Infrastructure Protection: Challenges in Securing Control Systems: Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform*, Report Number GAO-04-140T, (Washington, DC: 1 October 2003), 1.

[10] John Moteff, *Critical Infrastructure: The National Asset Database*, Report Number RL33648, Congressional Research Service Report for Congress, 16 July 2007, 4.

[11] Moteff, *Critical Infrastructure: The National Asset Database*, 1.

[12] Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, William Young, "Sustainable Security for Infrastructure SCADA," Report SAND2003-4670C, (Albuquerque, NM: Sandia National Laboratories, 2003), 1.

[13] Brian Krebs, Cyber Incident Blamed for Nuclear Power Plant Shutdown, *Washington Post*, 5 June 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html (accessed 17 December 2008).

[14] Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, Report Number RL31534, Congressional Research Service Report for Congress, 20 January 2004, 4.

[15] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Net," *The Register*, 20 August 2003, http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/(accessed 17 December 2008).

[16] Eric Byres, Justin Lowe, *The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems,* Technical Support Working Group, (Washington DC: 4 October 2004), 3.

[17] Ibid., 3.

[18] Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, 10.

[19] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare,* 40.

[20] Stephen M. Specht, Ruby B. Lee, *Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures,* Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, September 2004, 1.

[21] IP Source Tracker, (San Jose, CA: Cisco Systems, 2008), http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ipst.html (accessed on 17 December 2008).

[22] Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution,* (grant no. 2003-TK-TX-0003, U.S. Dept. of Homeland Security, Science and Technology Directorate, January 2008), 17.

[23] John Rollins, Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Congressional Research Service Report for Congress, updated 22 January 2007, 5.

[24] U.S. Supreme Court, Dalia v. United States, 441 U.S. 238 (1979), Argued January 9, 10, 1979, Decided April 1, 1979, 441 U.S. 238, *See Dalia*, 441 U.S. at 250 n.9, 252 n.13. http://supreme.justia.com/us/441/238/case.html (accessed 17 December 2008).

[25] *Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.* United States Code. Title 18, Part I, Ch 119, Sec 2511, para. (2)(a)(i).
http://www4.law.cornell.edu/uscode/18/2511.html (accessed 17 December 2008).

[26] Hunker, Hutchinson, Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution*, 13.

[27] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001*, HR 3162, 107th Cong., 1st sess., (October 26, 2001): Public Law 107-56, http://www.fincen.gov/statutes_regs/files/hr3162.pdf (accessed 17 December 2008).

[28] Ibid., 47.

[29] Department of Homeland Security, 2006 NIPP, 143.

[30] Office of Management and Budget, *OMB Reports Significant HSPD-12 Implementation Progress but Areas for Improvement Identified*, OMB Communications, 202-395-7254, (Washington DC: Office of Management and Budget, 31 October 2008), http://www.whitehouse.gov/omb/pubpress/2008/103108_hspd12.html (accessed 17 December 2008).

[31] Charter of the United Nations: Article 2(4), June 26, 1945, http://www.yale.edu/lawweb/avalon/un/unchart.htm#art2 (accessed on 1 February 2009)

[32] Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, *Information Warfare and International Law*, (Washington DC: National Defense University Press, 1998), 9.

[33] Ibid., 27.

[34] Mark C. Montgomery, *Cyber Threats: Developing a National Strategy for Defending Our Cyberspace*, (13 April 2000, repr., Cambridge MA: Program on Information Resources Policy, Harvard University, July 2001), 7.

[35] Thomas C. Wingfield, James B. Michael, *An Introduction to Legal Aspects of Operations in Cyberspace*, (Naval Postgraduate School: Monterey, CA, 28 April 2004), 13.

[36] Ibid,. 13.

[37] Michael G. Mullen, "From the Chairman, It's Time for a New Deterrence Model," *Joint Forces Quarterly*, Issue 51, 4th Quarter 2008, http://www.ndu.edu/inss/Press/jfq_pages/i51.htm (accessed 1 February 2009), 3.

[38] Gabriel Weimann, *Terror on the Internet, The New Arena, the New Challenges*, (Washington DC: United States Institute of Peace, 2006), 151.

[39] Ibid., 151.

[40] Khaled al-Faram, "Researcher: Al-Qaida-linked Web sites number 5,600," (ZDNet News, 4 December 2007), http://news.zdnet.com/2100-9588_22-178795.html (accessed 17 December 2008).

[41] United States Government Accountability Office, Information Security, *TVA Needs to Address Weaknesses in Control Systems and Networks*, Report Number GAO-08-526, (Washington, DC: May 2008), 8.

[42] Ibid., 8.

[43] Miniwatts Marketing Group, (Bogota, Colombia: 1997-2008), http://internetworldstats.com/middle.htm (accessed on 17 December 2008).

[44] Ibid.

[45] Gabriel Weimann, *www.terror.net How Modern Terrorism Uses the Internet*, special report 116, (Washington DC: United States Institute of Peace, March 2004), 6.

[46] Jialun Qina, Yilu Zhoub, Edna Reidc, Guanpi Laid, Hsinchun Chen, "Analyzing terror campaigns on the Internet: Technical sophistication, content richness, and Web interactivity," *International Journal of Human-Computer Studies*, 65 (2007): 71-84, 71.

[47] Statement of J. Michael McConnell, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*, (Washington, DC: 7 February 2008), 15.

[48] Scott Henderson, "Beijing's Rising Hacker Stars, How Does Mother China React?," *IO Sphere*, Fall 2008, 23.

[49] Ibid., 23.

[50] Ibid., 24.

[51] Ibid., 24.

[52] Ibid., 27.

[53] Emerging Cyber Threats Report for 2009, *Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond*, Georgia Tech Information Security Center (October 15, 2008), http://gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (accessed on 17 December 2008), 2.

[54] Dawn S. Onley, Patience Wait, *Red storm rising, DOD's efforts to stave off nation-state cyberattacks begin with China*, (Government Computer News, 21 Aug**ust** 2006), http://www.gcn.com/print/25_25/41716-1.html (accessed on 17 December 2008).

[55] Annual Report to Congress, *Military Power of the People's Republic of China 2007*, 21.

[56] Ibid., 11.

[57] Ibid., 22.

[58] Dean Takahashi, "After the five-day Russia-Georgia war, a chronicle of the cyber battle unfolds," (12 August 2008), http://venturebeat.com/2008/08/12/after-a-five-day-war-a-chronicle-of-the-cyber-battle-unfolds/ (accessed on 17 December 2008).

[59] Emerging Cyber Threats Report for 2009, *Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond*, 3.

[60] Charles Billo, Welton Chang, *Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States*, (Hanover, NH: Institute for Security Technology Studies, Dartmouth College, Revised December 2004), 114.

[61] Ibid., 115.

[62] Michael G. Mullen, "From the Chairman, It's Time for a New Deterrence Model," 2.

[63] Frank Kramer, Stuart Starr, Larry Wentz, Eli Zimet, Daniel Kuehl, *Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower*, 12th ICCRTS Adapting C2 to the 21st Century, Track: C2 Concepts, Theory, and Policy, 3.

[64] Statement of Jess T. Ford, Before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee on Appropriations, *U.S. Public Diplomacy, State Department Efforts Lack Certain Communication Elements and Face Persistent Challenges*, Report number GAO-06-707T, (Washington, DC: 3 May 2006), 2.

[65] Roy Schmadeka, "The War of Ideas: The Unheard Voice," *IO Sphere*, Fall 2008, 10.

[66] Field Manual (FM) 3-24, "Counterinsurgency", (Washington, DC: Depart. of the Army, 2006), 5-21.

[67] Peter W. Singer, "American Goodwill, in Shackles," (Washington, DC: Brookings Institution, 26 June 2007), http://www.brookings.edu/opinions/2007/0626islamicworld_singer.aspx, (Accessed on 20 January 2009).

[68] Norman Vasu, *The London Bombings: Fundamental Change in Fundamentalist Times*, (IDSS Commentaries no. 47, 28 July 2005), 3.

[69] Radical Middle Way, "About Us", www.radicalmiddleway.co.uk (accessed on 17 December 2008).

[70] Mohamed Bin Ali, *De-Radicalisation Programmes: Changing Minds*?, (RSIS Commentary No. 100, 23 September 2008), 2.

[71] Roy Schmadeka, "The War of Ideas: The Unheard Voice," 8.

[72] Ibid., 9.

[73] Ibid., 9.

[74] Ibid., 10.

[75] Weimann, *www.terror.net How Modern Terrorism Uses the Internet*, 7.

[76] Ibid., 7.

[77] United States: Report on the Observance of Standards and Codes-FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism, IMF Country Report No. 06/432, (Washington DC: International Monetary Fund, December 2006), 3.

[78] Ibid., 3.

[79] Weimann, *Terror on the Internet, The New Arena, the New Challenges*, 132.

[80] James Jay Carafano, "U.S. Thwarts 19 Terrorist Attacks Against America Since 9/11," *Backgrounder*, no. 2085, (Washington DC: The Heritage Foundation, 13 November 2007), http://www.heritage.org/research/HomelandDefense/bg2085.cfm#_ftn20 (accessed on 17 December 2008).

[81] Eric Swedlund, "UA effort sifting Web for terror-threat data," *Arizona Daily Star*, 24 September 2007, http://ai.arizona.edu/recognition/uadailystart.pdf (accessed 17 December 2008).

[82] The National Security Strategy of the United States of America, March 2006, 40.

[83] Ibid., 39.

[84] Dan Blumenthal, Randall Schriver, "Strengthening Freedom in Asia, A Twenty-First-Century Agenda for the U.S.-Taiwan Partnership," (Washington DC**:** The American Enterprise Institute, 22 February 2008), 2.

[85] Ibid., 8.

[86] Kelly Jackson Higgins, "Taiwan Says China Accounts For Most Cyber Attacks, Information Week," 17 January 2008, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=208803769 (accessed on 1 December 2008).

[87] Annual Report to Congress, *Military Power of the People's Republic of China 2007*, 7.

[88] Ibid., 8.

[89] Abram N. Shulsky, *Deterrence Theory and Chinese Behavior*, (Arlington, VA : RAND, Project Air Force, 1999-2003), 27.

[90] John J. Tkacik, Daniella Markheim, "Free Trade with Taiwan Is Long Overdue," *Backgrounder*, no. 2061, (Washington, DC: The Heritage Foundation, 15 August 2007), 2.

[91] Tkacik, Markheim, "Free Trade with Taiwan Is Long Overdue," 5.

[92] Correspondents in Kuala Lumpur, "Region hatches cyber defence," *Australian IT*, 31 July 2006, http://www.australianit.news.com.au/story/0,24897,19966914-15331,00.html, (accessed on16 January 2009).

[93] Maria Consuelo C. Ortuoste, *Reviewing the ASEAN Regional Forum and its Role in Southeast Asian Security*, Asia-Pacific Center for Security Studies (Honolulu, HI: February 2000).

[94] Richard Bassett, Vincent Ierace, Ellen Murphy, Riccardo Palmerini, "Security Risks Associated with Geosourcing," *The ISSA Journal*, September 2004, 2.

[95] Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, Report Number RL32114, Congressional Research Service Report for Congress, 17 October 2003, 22.

[96] Jennifer H. Svan, David Allen, "DOD bans the use of removable, flash-type drives on all government computers," *Stars and Stripes*, 21 November 2008, http://www.stripes.com/article.asp?section=104&article=58951 (accessed on 17 December 2008).

[97] Brig Gen William T. Lord, *U.S. Air Force Concept of Operations for Information Operations*, 6 February 2004, 9-10.

[98] *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*, National Security Agency/Central Security Service, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed on 07 February 2008).

[99] Department of Homeland Security, Control Systems Cyber Security: Defense in Depth Strategies, External Report # INL/EXT-06-11478, (Idaho National Laboratory, May 2006), 19.

[100] Ibid., 21.

[101] Charlotte Adams, "Securing Information Vexes Defense Planners," *Signal Magazine*, vol. 63 no. 3, November 2008, 105.

[102] Ibid., 105.

[103] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare,* 65.

[104] Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, (Washington, DC: Center for Strategic and International Studies, December 2008, 62.

[105] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,* Special Report CMU/SEI-2002-SR-009, (Pittsburgh, PA: Carnegie-Mellon ZSoftware Engineering Institute, November 2002), 20.